

After the title and before the first paragraph on page 1, insert the following heading at the left-hand margin:

FIELD OF THE INVENTION

Page 1, line 7, insert a paragraph indentation before the sentence beginning "More precisely,..." and insert the following heading at the left-hand margin:

BACKGROUND OF THE INVENTION

Page 1, line 21, delete "We are" and substitute -The invention herein is--;

Page 1, line 22, before "algorithms", insert -cryptographic--;

Page 1, at line 26, before the paragraph beginning "Attacks,...", insert the following heading at the left hand margin:

DESCRIPTION OF RELATED ART

Page 1, line 30, before "incorporated", insert -the subject matter of which is hereby--;

Page 2, line 7, delete "we will consider";

Page 2, line 8, after "algorithm", delete ", a description of which", and substitute -will be considered. A description--;

Page 9, line 17, in the second equation, delete "to" and substitute -into--;

Page 9, line 18, in the equation, delete "to" and substitute -into--;

Page 12, at line 5, and before the paragraph beginning "One of the objects of the ..." insert the following paragraph at the left-hand margin:

SUMMARY OF THE INVENTION

Page 15, at line 26 and before the paragraph beginning "Other characteristics and advantages ...", insert the following heading at the left hand margin:

BRIEF DESCRIPTION OF THE DRAWINGS

Page 16, at line 14 and before the paragraph beginning "The invention...",
insert the following heading at the left hand margin:

AL6 /DESCRIPTION OF THE PREFERRED EMBODIMENT(S)/

Page 20, after line 18, insert the following new paragraph:

A7 /While this invention has been described in conjunction with specific
embodiments thereof, it is evident that many alternatives, modifications and
variations will be apparent to those skilled in the art. Accordingly, the preferred
embodiments of the invention as set forth herein, are intended to be illustrative, not
limiting. Various changes may be made without departing from the true spirit and full
scope of the invention as set forth herein and defined in the claims./